AMENDMENTS TO THE CLAIMS

Please cancel claims 1, 8, 14, 20, 26 without prejudice and accept amended claims 2-7, 9-13, 15-19, 21-25, 27-34 as follows:

1. (Cancelled)

2. (Currently Amended) The system as recited in claim ~~1~~5, wherein the steganographic unit employs a steganographic masking algorithm.

3. (Currently Amended) The system as recited in claim ~~1~~5, wherein the data stream includes a transmission order which alternates between first units and second units.

4. (Currently Amended) The system as recited in claim ~~1~~5, wherein the steganographic unit encrypts the at least one second unit.

5. (Currently Amended) ~~The system as recited in claim 1~~ A system for enforcing data stream continuity comprising:

a server coupled to a transmission link for providing a data stream to at least one client over the transmission link, the data stream being segmented into units, the server including:

a scrambler for encrypting at least one first unit using an encryption key;

a steganographic unit for embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by the client to determine the encryption key and decipher the data stream,

wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

6. (Currently Amended) The system as recited in claim ~~1~~5, wherein the transmission link includes the Internet.

7. (Currently Amended) The system as recited in claim ~~1~~5, wherein at least one of the client and the server include a memory storage device.

8. (Cancelled)

9. (Currently Amended) The system as recited in claim ~~8~~11, wherein the data stream includes a transmission order which alternates between first units and second units.

10. (Currently Amended) The system as recited in claim ~~8~~11, wherein the encryption key is also steganographically hidden in the at least one second unit.

11. (Currently Amended) ~~The system as recited in claim 8~~ A system for enforcing data stream continuity comprising:

a client system coupled to a transmission link for receiving a data stream from at least one server over the transmission link, the data stream being segmented into units, the client system including:

a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server such that steganographic information is needed by the client to determine the encryption key;

a descrambler for descrabling at least one second unit which was encrypted in accordance with the encryption key before transmission from the server; and

a decoder coupled to the key extractor and the descrambler for reassembling the data stream such that all of the units of the data stream are needed to decipher the data stream,

wherein that at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

12. (Currently Amended) The system as recited in claim ~~8~~11, wherein the transmission link includes the Internet.

13. (Currently Amended) The system as recited in claim ~~8~~11, wherein at least one of the client and the server include a memory storage device.

14. (Cancelled)

15. (Currently Amended) The method recited in claim ~~14~~17, wherein the data stream includes a transmission order which alternates between first units and second units.

16. (Currently Amended) The method as recited in claim ~~14~~17, wherein the step of steganographically embedding includes the step of steganographically embedding portions of the encryption key in the at least one first unit.

17. (Currently Amended) ~~The method as recited in claim 14~~ A method for enforcing data stream continuity comprising the steps of:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key;

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream;

extracting the encryption key steganographically embedded in at least one second unit in the data stream;

descrabling at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream,

wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

18. (Currently Amended) The method as recited in claim ~~14~~17, wherein the transmission link includes the Internet.

19. (Currently Amended) The method as recited in claim ~~14~~17, wherein at least one of the client and the server include a memory storage device.

20. (Cancelled)

21. (Currently Amended) The method recited in claim ~~20~~23, wherein the data stream includes a transmission order which alternates between first units and second units.

22. (Currently Amended) The method as recited in claim ~~20~~23, wherein the step of steganographically embedding includes the step of steganographically embedding portions of the encryption key in the at least one first unit.

23. (Currently Amended) ~~The method as recited in claim 20~~ A method for enforcing data stream continuity comprising the steps of:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key;

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream,

wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

24. (Currently Amended) The method as recited in claim ~~20~~23, wherein the transmission link includes the Internet.

25. (Currently Amended) The method as recited in claim ~~20~~23, wherein at least one of the client and the server include a memory storage device.

26. (Cancelled)

27. (Currently Amended) The method recited in claim ~~26~~29, wherein the data stream includes a transmission order which alternates between first units and second units.

28. (Currently Amended) The method as recited in claim ~~26~~29 wherein the portions of the encryption key are embedded in the at least one first unit.

29. (Currently Amended) ~~The method as recited in claim 26~~ A method for enforcing data stream continuity comprising the steps of:

providing data segmented into units for a data stream transferred over a link, the units including at least one first unit and at least one second unit;

extracting an encryption key steganographically embedded in at least one second unit in the data stream;

descrabling the at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream,

wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

30. (Currently Amended) The method as recited in claim ~~26~~29, wherein the link includes the Internet.

31. (Currently Amended) The method as recited in claim ~~26~~29, wherein at least one of the client and the server include a memory storage device.

32. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform methods steps for enforcing data stream continuity, the methods steps comprising:

segmenting data to be transmitted over a link into units for a data stream to be transferred over a link;

scrambling at least one first unit for the data stream before transmission by encrypting the at least one first unit using an encryption key;

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream;

extracting the encryption key steganographically embedded in at least one second unit in the data stream;

descrabling at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream,

wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

33. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform methods steps for enforcing data stream continuity, the methods steps comprising:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key; and

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream,

wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

34. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform methods steps for enforcing data stream continuity, the methods steps comprising:

providing data segmented into units for a data stream transferred over a link, the units including at least one first unit and at least one second unit;

extracting an encryption key steganographically embedded in at least one second unit in the data stream;

descrabling the at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream,

wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.